Les quatre premières parties du problème sont largement indépendantes.

Partie I

Dans cette partie I, on étudie une méthode de calcul de l'inverse d'un élément a d'un groupe multiplicatif G de cardinal fini $N \in \mathbb{N}^*$. L'élément neutre de G est noté 1.
« Écrire un algorithme » signifie le rédiger en français, sous une forme rappelant un programme d'un langage tel que Pascal, Maple, Matlab, etc.
Le coût d'un algorithme est le nombre de multiplications dans le groupe G que nécessite son exécution. On ne tiendra pas compte des autres opérations (en particulier celles dans $\mathbb{N}$).

1. Justifier le fait que a^{N-1} est inverse de a dans G.
2. On écrit la décomposition en base 2 de $N-1$ sous la forme :
$$N-1 = \sum_{i=0}^{k} x_i 2^i \text{ avec } k \in \mathbb{N},\ x_i \in \{0,1\} \text{ pour } i \in [\![0,k]\!] \text{ et } x_k \neq 0.$$
On considère les suites finies $(a_i)_{0 \leqslant i \leqslant k+1}$ et $(b_i)_{0 \leqslant i \leqslant k+1}$ définies par :
$$a_0 = 1,\ b_0 = a \text{ et pour } i \in [\![0,k]\!],\ a_{i+1} = a_i b_i^{x_i},\ b_{i+1} = b_i^2.$$
   a) Démontrer que a_{k+1} est l'inverse de a dans G.
   b) En déduire un algorithme de calcul de a^{-1} et préciser, en fonction de k, son coût dans le pire des cas (c'est-à-dire le nombre maximum de multiplications dans G que nécessite le calcul de a^{-1} ; on ne tiendra pas compte du coût éventuel du calcul des x_i, $0 \leqslant i \leqslant k$). L'algorithme doit prendre comme arguments a et N.
3. **Exemple.** Dans cette question, G est le groupe des éléments inversibles de $\mathbb{Z}/148\mathbb{Z}$. On note encore a la classe dans $\mathbb{Z}/148\mathbb{Z}$ d'un élément a de $\mathbb{Z}$.
   a) Déterminer le cardinal N de G.
   b) Démontrer que 5 est un élément de G et déterminer son inverse par la méthode de la question I.2.
   c) Donner une autre méthode pour déterminer cet inverse.

Partie II

1. a) Soit π un élément d'un groupe multiplicatif G, e un entier relatif et $\alpha = \pi^e$.
   On considère l'application f_α de $\mathbb{Z} \times G$ dans G^2 définie par $f_\alpha(k,\tau) = (\pi^k, \tau\,\alpha^k)$.
   Exhiber une fonction φ_e de G^2 dans G, ne dépendant que de e et vérifiant
   $$\tau = \varphi_e \circ f_\alpha(k,\tau) \text{ pour tout } (k,\tau) \in \mathbb{Z} \times G.$$
   b) On suppose le groupe G et l'élément π connus de tous les membres d'une association. L'un d'eux, **A**, garde secret l'entier e et rend public l'élément $\alpha = \pi^e$, ainsi donc que la fonction f_α. On recherche une procédure permettant à chacun d'envoyer à **A** un message crypté sous la forme d'un (ou de plusieurs) élément(s) τ de G, telle que la seule connaissance de e suffise à retrouver le message initial.
   Justifier le fait que, si l'auteur décompose son message en parties telles que chacune puisse être représentée par un élément τ_i du groupe, choisit pour chacune d'elles un entier k_i et envoie les couples $f_\alpha(k_i, \tau_i) = (\lambda_i, \mu_i)$ à **A**, alors ce dernier peut les décrypter grâce à φ_e.

2. Dans cette question, G est le groupe $\mathbb{F}_{29}^*$ des inversibles du corps à 29 éléments et les nombres $\pi = 2$ et $\alpha = 18$ sont supposés publics.

   Chaque associé sait que les entiers (1, 2, …, 26, 27, 28) modulo 29, dans cet ordre, représentent les éléments du 28-uplet (`A`, `B`, …, `Z`, ‘ ’, ·), où ‘ ’ figure l'espace séparant deux mots et · est le point de fin de phrase.

   a) Sachant que l'algorithme de décryptage employé par **A** repose sur la seule table ci-dessous des résidus modulo 29 des puissances dix-septièmes des entiers entre 2 et 28 :

λ	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
λ^{17}	21	2	6	9	13	24	10	4	15	3	12	22	11	18	7	17	26	14	25	19	5	16	20	23	27	8	28

   conjecturer la valeur de e et la contrôler grâce à α.

   b) Décrypter le message suivant (on donne la suite des couples $\big((\lambda_i, \mu_i)\big)$:

   (16, 17), (18, 24), (28, 22), (17, 21), (23, 23), (24, 8).

Partie III

Dans cette partie III, le corps de base est le corps fini $\mathbb{F}_{16}$ *à* 16 *éléments, unique à isomorphisme près.*

1. a) Comment peut-on construire $\mathbb{F}_{16}$?

   b) Démontrer que le groupe multiplicatif $\mathbb{F}_{16}^*$ est formé des puissances successives d'un élément ω vérifiant l'égalité $\omega^4 + \omega^3 + 1 = 0$.

   c) Démontrer que ω, ω^2, ω^4 et ω^8 sont les racines du polynôme $X^4 + X^3 + 1$ dans $\mathbb{F}_{16}$.

   d) Démontrer que la famille $(\omega, \omega^2, \omega^4, \omega^8)$ est une base de $\mathbb{F}_{16}$ sur $\mathbb{F}_2$.

2. a) Soit $a \in \mathbb{F}_{16}$. Résoudre dans $\mathbb{F}_{16}$ l'équation $x^5 = a$, en discutant éventuellement selon la valeur de a.

   b) Démontrer qu'il existe quatre éléments $\gamma \in \mathbb{F}_{16}$ tels que, pour chacun d'eux, la famille $(\gamma, \gamma^2, \gamma^4, \gamma^8)$ est une base de $\mathbb{F}_{16}$ sur $\mathbb{F}_2$ telle que le produit de deux de ses éléments appartient à la base ou est égal à 1.

   Expliquer rapidement pourquoi les calculs dans $\mathbb{F}_{16}$ sont plus faciles dans une telle base.

Partie IV

Une *cubique* sur un corps $\mathbb{K}$ est l'ensemble Γ des points $M = (x, y) \in \mathbb{K}^2$ annulant un polynôme du troisième degré $P(X,Y) = a\,X^3 + b\,X^2Y + c\,XY^2 + d\,Y^3 + e\,X^2 + f\,XY + g\,Y^2 + h\,X + i\,Y + j$ à coefficients dans $\mathbb{K}$.

Dans toute la suite, P est supposé non nul.

Remarque : il existe plusieurs polynômes donnant le même sous-ensemble de $\mathbb{K}^2$, comme le montre l'exemple des polynômes XY^2 et X^2Y. Il est systématiquement sous-entendu que l'on a fait un choix particulier de P (ou de l'un de ses produits par les éléments de $\mathbb{K}^*$).

Cette partie étudie quelques cubiques particulières sur le corps $\mathbb{R}$.

1. Dans cette question, on prend la cubique Γ définie par le polynôme $P = X^3 - Y \in \mathbb{R}[X, Y]$.

   a) La tracer à main levée.

b) Démontrer que toute droite coupe Γ en exactement un ou trois points en comptant leur multiplicité éventuelle et que, lorsqu'il existe trois points d'intersection notés $A = (x_A, y_A)$, $B = (x_B, y_B)$, $C = (x_C, y_C)$:

$$x_A + x_B + x_C = 0.$$

On note Ω le point de coordonnées $(0, 0)$ de Γ. Pour tout couple (A, B) de points de Γ, on considère le troisième point C d'intersection avec Γ de la droite AB (ou de la tangente en A à Γ si $B = A$), puis le troisième point d'intersection $A * B$ de la droite ΩC avec Γ. Ceci définit sur Γ une loi multiplicative $*$ (on peut compléter le dessin du IV.1.a).

c) Démontrer que $(\Gamma, *)$ est un groupe isomorphe à $(\mathbb{R}, +)$.

2. Reprendre la question 1. pour $P = X^3 - 3\,XY - 1 \in \mathbb{R}\,[X, Y]$ et $\Omega = (1, 0)$, en précisant à quel groupe usuel est isomorphe $(\Gamma, *)$ dans cet exemple.
3. On étudie dans la suite des cubiques du plan projectif.
   On considère un polynôme non nul homogène à trois variables :

$$\overline{P}\,(X, Y, Z) = a\,X^3 + b\,X^2Y + c\,XY^2 + d\,Y^3 + e\,X^2Z + f\,XYZ + g\,Y^2Z + h\,XZ^2 + i\,YZ^2 + jZ^3.$$

   La cubique associée est l'ensemble Γ des points du plan projectif dont les coordonnées homogènes (X, Y, Z) vérifient $\overline{P}(X, Y, Z) = 0$.
   Démontrer que l'intersection de Γ avec toute droite du plan projectif est constituée d'exactement un ou trois points, en comptant toujours les multiplicités éventuelles.
4. Dans cette question 4, on considère $P = Y^3 - X^2 - Y^2$ et le polynôme homogène associé $\overline{P}(X, Y, Z) = Y^3 - X^2Z - Y^2Z$.

   a) Dans cette question 4.a, on se place dans le plan affine euclidien $\mathbb{R}^2$ et on considère la courbe γ d'équation $y^3 = x^2 + y^2$ privée du point $(0, 0)$.
   En choisissant un paramétrage de γ (par exemple en coordonnées polaires), étudier cette courbe et la tracer, en précisant l'allure des branches infinies s'il en existe.
   On ne demande pas d'étudier les éventuels points d'inflexion.

Dans la suite de la question 4., on considère dans le plan projectif la cubique Γ *d'équation* $Y^3 - X^2Z - Y^2Z = 0$, *privée du point de coordonnées* $(0, 0, 1)$.
On choisit pour Ω *le point à l'infini* $(1, 0, 0)$ *et on définit le composé* $A * B$ *de deux points quelconques de* Γ *comme en IV.1.*

   b) Montrer que Γ admet comme paramétrage :

$$\begin{cases} X = \cos\theta \\ Y = \sin\theta \\ Z = \sin^3\theta \end{cases} \qquad \theta \text{ décrivant } \mathbb{R}.$$

   Si A et B sont deux points de Γ, caractériser le point C tel que $C = A * B$.

   c) Démontrer que $(\Gamma, *)$ est isomorphe à un groupe usuel que l'on précisera.
   Quels sont les points d'ordre 6 ?

Partie V

Dans cette partie V, on étudie la courbe Γ' définie dans le plan $\mathbb{F}_{16}^2$ par l'équation :

$$y^2 + y = x^3 + x.$$

1. Montrer que la courbe Γ' contient au plus 32 points de $\mathbb{F}_{16}^2$.
2. On introduit le polynôme homogène

$$\overline{P}(X, Y, Z) = X^3 + XZ^2 - Y^2Z - YZ^2$$

   Définir, par analogie avec la partie IV, un point à l'infini Ω et une multiplication interne à l'ensemble Γ réunion de Γ' et de Ω.

3. a) Montrer que cette multiplication, notée $*$, est commutative et admet un élément neutre, vis-à-vis duquel tout point admet un inverse.
   b) Calculer l'inverse d'un élément $A = (\alpha, \beta)$ de Γ'.

On admettra que cette loi est associative et munit donc Γ d'une structure de groupe commutatif.

4. On se propose de calculer le carré $A^2 = A * A$ d'un élément $A = (\alpha, \beta)$ de Γ'.
   On est amené à considérer la droite D passant par A telle que son intersection avec Γ' admet A comme point double.
   a) Montrer que cette droite – appelée tangente en A à la courbe Γ' – a pour équation

$$P'_X(\alpha, \beta)(x - \alpha) + P'_Y(\alpha, \beta)(y - \beta) = 0$$

   où P'_X et P'_Y désignent les polynômes dérivés du polynôme P, respectivement par rapport à X et Y.
   b) Déterminer les coordonnées de $A * A$.
   c) En déduire que, pour tout point A de Γ' : $A^4 = A^{-1}$.
   d) En déduire le cardinal de Γ et sa décomposition en produit direct de groupes cycliques.

5. Indiquer brièvement comment implanter un système de cryptographie du type de celui de la partie II à l'aide de Γ.